GAO
Global Access Operations
The mission never sleeps...

BOUNDLESSINFORMANT

Describing Mission Capabilities from Metadata Records

[redacted]

13 July 2012

THE QUESTION

(U//FOUO) How do we describe the collection capabilities and posture of our SIGINT infrastructure?

The Old Way

(U//FOUO) Typical SIGINT Data Calls/Questions

1. How many sites do we have in the region? How many records are they producing?
2. What type of coverage do we have on country X?
3. What type of collection and volume do we get out of site A? How do these types/volumes compare against site B? Against site C?

(U//FOUO) Ways to Get Answers

1. Map out the physical location of SIGINT assets
2. Send out a data call based on best guesses for who can answer the question
3. Review static reports/spreadsheets from previous data calls
4. Ask a 30-year SIGINTer

THE NEW WAY *BOUNDLESSINFORMANT*

(U//FOUO) Use Big Data technology to query SIGINT collection in the cloud to produce near real-time business intelligence describing the agency's available SIGINT infrastructure and coverage.

(U//FOUO) Key Questions

1. How many records are collected for an organizational unit (e.g. FORNSAT) or country?
2. Are there any visible trends?
3. What assets collect against a specific country? What type of collection?
4. What is the field of view for a specific site? What type of collection?

(U//FOUO) Potential Users

1. Strategic decision makers (leadership team)
2. Tactical users (mission and collection managers)

DETAILS

1) (U//FOUO) Current focus is on SIGINT/COMINT

2) (U//FOUO) Review every valid DNI and DNR metadata record passing through the NSA SIGINT infrastructure

   a) (U//FOUO) For the Map View, only display aggregated counts of records with a normalized number or an administrative region populated.

   b) (U//FOUO) For the Org View, display aggregated counts of every valid record.

3) (U//FOUO) Raw data, analytics, and back-end database are all conducted in the cloud (HDFS, MapReduce, Cloudbase).

(U//FOUO) BOUNDLESSINFORMANT is hosted entirely on corporate services and leverages FOSS technology (i.e. available to all NSA developers).

DEMO


BOUNDLESSINFORMANT
Collection Information
Alarm Summary
Total Collection - Last 7 Days
Signal Profile
Most Volume

Road Map

1) (U//FOUO) Add technology type (e.g. JUGGERNAUT, LOPER) to provide additional granularity in the numbers

2) (U//FOUO) Integrate Site Similarity capability (i.e. Gephi Charts)

3) (U//FOUO) Anomaly detection and alerts

4) (U//FOUO) Other "INT" data (e.g. ELINT, FISINT)

5) (U//FOUO) Add survey data and display delta between collected metadata and survey data

6) (U//FOUO) Add in selected (vs. unselected) data indicators